FAQ zur Datenschutz-Grundverordnung

Was sind die wesentlichen Neuerungen durch die DSGVO?

a) Erweiterter Geltungsbereich

Die DS-GVO betrifft Unternehmen in der gesamten EU und deckt alle Bereiche der EU-Gesetzgebung ab, unabhängig von:

- Datenformat,
- Ort des Datensubjekts,
- Sitz des Unternehmens, dass die Daten sammelt oder verarbeitet,
- Nationalität des Datensubjekts.

b) Umfassendere Definitionen datenschutzrelevanter Begrifflichkeiten

- Klarstellung zu persönlichen Identifiern im Anwendungsbereich der Datenschutzgesetze (z. B. Name, Geolokalisierung, Online Identifizierung, Passwörter, genetische Daten, etc.),
- Begriffsbestimmung für genetische und biometrische Daten in Kombination mit speziellen Regelungen zu Gesundheitsdaten,
- spezielle Regelung und Vorgaben zur Pseudonymisierung personenbezogener Daten.

c) Weitreichendere Rechte für die betroffenen Personen

Neue und teils stärker ausdifferenzierte Betroffenenrechte wie z. B. das Recht auf Datenportabilität sowie ein generelles Widerspruchsrecht gegen alle Formen der Datenverarbeitung (jedoch nur unter gewissen Voraussetzungen).

d) Erweiterte Haftung für Auftragsverarbeiter

- Mitverantwortlichkeit des Auftragsverarbeiters bei Auslagerung der Verarbeitungsprozesse gegenüber den Betroffenen,
- Mithaftung des Auftragsverarbeiters gegenüber Betroffenen sowie Behörden (Bußgeld).

e) Verschärfte Sanktionen

- Deutlich mehr sanktionierbare Verstöße,
- deutlich erhöhte Geldbußen.

Für wen gilt die neue Datenschutz-Grundverordnung?

Örtlich gilt die DSGVO für alle Unternehmen, die

- in der EU ansässig sind,
- im osteuropäischen Ausland ansässig sind, und betroffenen Personen, die sich innerhalb der EU bzw. des EWR befinden, Waren oder Dienstleistungen anbieten, unabhängig davon, ob von den betroffenen Personen eine Zahlung zu leisten ist, und/oder das Verhalten betroffener Personen im EWR beobachten, soweit ihr Verhalten in der Union erfolgt.

Persönlich findet die DSGVO Anwendung auf Behörden und Unternehmen sowie Einzelpersonen, die personenbezogene Daten zu nicht ausschließlich persönlichen oder familiären Tätigkeiten verarbeiten. Dabei finden die Regelungen nur Anwendung auf das „Erheben“ und „Verarbeiten“ von personenbezogenen Daten, was die ganz oder teilweise automatisierte Verarbeitung sowie die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, umfasst.

Was sind personenbezogene Daten?

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, z.B. Name, Adresse, Telefonnummer, Autokennzeichen, aber auch Online Kennungen (wie z.B. die IP-Adresse). Es ist ausreichend, wenn die Information zu einer Person in irgendeiner Art zugeordnet und somit ein Personenbezug hergestellt werden kann.

Welche Grundsätze sind bei der Umsetzung der Datenschutz-Grundverordnung zu beachten?

Die Datenschutz-Grundverordnung verlangt erhöhte Dokumentations- und Nachweispflichten und verpflichtet datenverarbeitende Unternehmen zur Einhaltung folgender definierter Grundsätze:

a) **Rechtmäßigkeit**, Verarbeitung nach Treu und Glauben, Transparenz: Verarbeitung auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise.

b) **Zweckbindung**: Datenerhebung für festgelegte, eindeutige und legitime Zwecke.

c) **Datenminimierung**: dem Zweck angemessene Datenerhebung und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt.

d) **Richtigkeit**: Daten sollen sachlich richtig und – wenn erforderlich – auf dem neuesten Stand sein; personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, sollen unverzüglich gelöscht oder berichtigt werden.

e) **Speicherbegrenzung**: die Identifizierung der betroffenen Personen soll nur so lange möglich sein, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

f) **Integrität und Vertraulichkeit**: Gewährleistung einer angemessenen Sicherheit der personenbezogenen Daten, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

Wann ist die Verarbeitung personenbezogener Daten rechtmäßig (Art. 6 Abs. 1 DSGVO)?

Auch die DSGVO folgt dem aus dem deutschen Recht bisher bekannten Prinzip des sogenannten „Verbotes mit Erlaubnisvorbehalt“. Dies besagt, dass eine Verarbeitung personenbezogener Daten nur dort zulässig ist, wo sie entweder im Wege einer Einwilligung des betroffenen oder eines ausdrücklichen gesetzlichen Erlaubnistatbestandes gestattet ist. Die Verarbeitung personenbezogener Daten ist insoweit rechtmäßig, wenn mindestens eine der folgenden Voraussetzungen vorliegt:

- Es liegt eine Einwilligung der betroffenen Person vor,
- die Datenverarbeitung ist zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen notwendig,
- die Datenverarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung nötig,
- die Datenverarbeitung ist zum Schutze lebenswichtiger Interessen nötig,
- die Datenverarbeitung ist zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt notwendig,
- die Datenverarbeitung ist aufgrund einer Interessenabwägung erforderlich.

Welche technischen Schutzmaßnahmen verlangt die DSGVO von Unternehmen?

Unternehmen, die Daten verarbeiten, müssen zunächst für geeignete technische und organisatorische Maßnahmen sorgen und interne Strategien festlegen sowie Maßnahmen treffen, die a) den Grundsatz des Datenschutzes durch Technik (privacy by design) entsprechen und b) datenschutzfreundliche Voreinstellungen (privacy by default) sicherstellen. Mögliche Maßnahmen hierzu können wie folgt lauten:

- Minimierung der Verarbeitung personenbezogener Daten,
- Pseudonymisierung personenbezogener Daten,
- Überwachung der Datenverarbeitung,
- Verbesserung der Sicherheitsfunktionen.

Zudem werden besondere Voraussetzungen an die Sicherheit der Verarbeitung personenbezogener Daten gestellt. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen haben verantwortliche Stellen (sowie Auftragsverarbeiter) geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessene Schutzniveau zu gewährleisten; diese Maßnahmen schließen u.A. folgendes mit ein:

- Minimierung der Verarbeitung personenbezogener Daten,
- Pseudonymisierung personenbezogener Daten,
- Überwachung der Datenverarbeitung,
- Verbesserung der Sicherheitsfunktionen.

Welche Angaben muss ein Verzeichnis von Verarbeitungstätigkeiten umfassen (Art. 30 DSGVO)?

Grundsätzlich hat jedes Unternehmen ein Verzeichnis aller Verarbeitungstätigkeiten zu führen. Dieses Verzeichnis muss folgende Angaben enthalten:

- Name und die Kontaktdaten des für die Verarbeitung Verantwortlichen (ggf. auch Vertreter und Datenschutzbeauftragter),
- Zweck der Verarbeitung,
- Kategorien von betroffenen Personen und personenbezogenen Daten,
- Kategorien von Empfängern, an die personenbezogene Daten weitergegeben worden sind oder noch weitergegeben werden (auch in Drittländern),
- Übermittlungen von Daten an ein Drittland oder an eine internationale Organisation,
- vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien,
- allgemeine Beschreibung der technischen und organisatorischen Maßnahmen.

Das Verzeichnis der Verarbeitungstätigkeiten ist u.A. ein wesentliches Instrument, um der Rechenschaftspflicht im Sinne von Art. 5 Absatz 2 DSGVO nachzukommen und insoweit den Nachweis darüber führen zu können, dass die Grundsätze für die Verarbeitung personenbezogener Daten (Art.5 DSGVO) eingehalten werden.

Wann ist eine Datenschutz-Folgenabschätzung nötig (Art. 35 DSGVO)?

Eine Datenschutz-Folgeabschätzung ist nötig, wenn eine Form der Verarbeitung wahrscheinlich ein hohes Risiko für die betroffenen Personen verursacht, insbesondere beim Einsatz neuer Technologien und aufgrund des Wesens, des Umfangs und des Kontextes sowie der Zwecke der in Rede stehenden Verarbeitungshandlung.

Dabei stellt sich oftmals die Frage, welche Technologien und/oder Verarbeitungsweisen hiervon erfasst sein können. Folgende Verarbeitungstätigkeiten können insoweit einer Datenschutzfolgenabschätzung unterliegen:

- Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen aufgrund automatisierter Verarbeitung,
- umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten,
- systematische weiträumige Überwachung öffentlich zugänglicher Bereiche.

Was ist die Aufgabe des Datenschutzbeauftragten und wann ist er nötig?

Die Aufgaben des Datenschutzbeauftragten lassen sich wie folgt zusammenfassen:

1. Unterrichtung und Beratung,
2. Überwachung der Einhaltung der Datenschutzvorschriften,
3. Beratung im Zusammenhang mit der Datenschutzfolgeabschätzung und Überwachung ihrer Durchführung,
4. Zusammenarbeit mit den Aufsichtsbehörden,
5. Tätigkeit als Anlaufstelle für die Aufsichtsbehörde.

Der Datenschutzbeauftragte steht dabei der verantwortlichen Stelle beratend zur Seite und unterstützt die Geschäftsleitung sowie die mit der Wahrnehmung entsprechender Aufgaben im Unternehmen betrauten Fachabteilung bei der Anwendung und Umsetzung der Datenschutzvorschriften. Ob ein Datenschutzbeauftragter bestellt werden muss, hängt von der Anzahl der Mitarbeiter, der Art der verarbeiteten personenbezogener Daten sowie dem Geschäftsfeld des Unternehmens ab. Ein Datenschutzbeauftragter muss deshalb dann bestellt werden, wenn im Unternehmen in der Regel mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Werden im Unternehmen dagegen Verarbeitungsvorgänge vorgenommen, die einer Datenschutzfolgeabschätzung nach Art. 35 DS-GVO unterliegen oder verarbeitet das Unternehmen personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung, hat das Unternehmen unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen einen Datenschutzbeauftragten zu benennen.

Wie können sich Unternehmen auf Daten-Vorfälle vorbereiten?

Jedes Unternehmen sollte zunächst Regeln aufstellen, an wen Datenschutz-Verletzungen intern d.h. innerhalb des Unternehmens, unter Einhaltung welcher Prozesse und Zeitlinien zu melden sind.

Zudem ist zu regeln, wer in die Aufklärung etwaiger Datenschutzvorfälle zu involvieren ist (interne/externe IT-Dienstleister und Forensiker, der Datenschutzbeauftragte oder weitere Verantwortliche des Unternehmens).

Zuletzt bedarf es der Dokumentation kritischer Systeme und Daten, um im Fall eines Datenschutzverstosses bzw. Datenschutzvorfalles schnell ermitteln zu können, ob etwaige Meldepflichten oder sonstige Verhaltenspflichten aus der DSGVO bestehen. Hintergrund ist, dass Meldepflichten (gegenüber der Behörde oder Betroffenen) regelmäßig nur bei besonderen Verarbeitungsvorgängen bestehen (bei denen die Gefahr für die Betroffenen als besonders hoch eingestuft wird).

Zu empfehlen ist weiterhin ein aktuell zu haltender und praxiserprobter Krisenplan, um im Krisenfall schnell die richtigen Schritte einleiten zu können und einen möglichen Datenschutzvorfall schnellstmöglich zu beherrschen und im Idealfall auch beheben zu können.

An wen muss eine Datenschutzverletzung gemeldet werden?

Sollte eine Datenschutzverletzung voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führen, ist diese nach Art. 33 DSGVO unverzüglich und möglichst innerhalb von 72 Stunden ab Kenntnis des Verstoßes an die zuständige Aufsichtsbehörde zu melden. Die Meldung muss mindestens die Beschreibung des Vorfalls, die Kontaktdaten der verantwortlichen Stelle, die wahrscheinlichen Folgen des Datenschutzvorfalls sowie eine Information über ergriffene Maßnahmen enthalten. Dabei sollten sich alle Unternehmen frühzeitig einen Überblick über die bei den jeweiligen Aufsichtsbehörden etablierten Meldeprozesse verschaffen, um im Ernstfall effizient mit der Behörde kommunizieren zu können.

Nach Art. 34 DSGVO besteht in entsprechenden Fällen zudem die Pflicht, unverzüglich eine Benachrichtigung der Betroffenen einzuleiten.

Aufgrund der weitreichenden Folgen eines Datenschutzverstoßes und der Meldung an Aufsichtsbehörden und Betroffene sowie die erheblichen Bußgeldandrohungen sollten die Voraussetzungen im Einzelfall stets genau beleuchtet werden.